UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/089,941	09/15/2003	Bruno Dutertre	SRI/4283-2	1672

52197 7590 01/11/2006

MOSER, PATTERSON & SHERIDAN, LLP
SRI INTERNATIONAL
595 SHREWSBURY AVENUE
SUITE 100
SHREWSBURY, NJ 07702

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 01/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/089,941	DUTERTRE ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 October 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on October 27, 2005.

Claims 1-18 are pending.

Response to Argument

2. Applicant's remark/arguments filed on October 27, 2005, have been fully considered but they are not persuasive.

Applicant's first argument is regarding the independent claims 1, 13,16 and 18

Applicant's argued that some of the limitation in the independent claims is not suggested by **the references** on the record, namely Aura.

Applicant wrote the following in support of his argument,

"Aura, only teaches a method for authenticating a mobile station, and does not teach the transmission of an encrypted message that includes a plurality of nonce values (e.g, a first nonce value and a second nonce value). At most Aura merely teaches a hash-based authentication protocol that uses two random numbers (RAND1 and RAND2) and a shared key (ki)."

Examiner disagrees with the above argument,

In response to the above argument by the applicant, the Examiner point out the following.

The nonce values as described in the disclosure are just numbers so the two random number recited in Aura (RAND1 and RAND2) indeed meets the limitation of the two nonce values of the application. With respect to the argument that Aura does not teach/disclose the transmission of an

encrypted message that includes a plurality of nonce values (e.g, a first nonce value and a second nonce value), the examiner would point out that Aura on column 6, lines 37-50 indeed discloses/teaches the following,

At stage 404 it generates the random number RAND2. The authentication key Ki and the random numbers RAND1 and RAND2 are entered at stage 405 as the starting data for the one-way hash functions H1, H2 and H3, which provide the following,

(1) SRES1=H1(Ki, RAND1, RAND2),

Algorithms H1 is one-way hash functions H(K,X1,X2) with key Ki."

Therefore the two nonce values RAND1 and RAND2 are indeed encrypted by the Key Ki using the Hash function H1 and the result of the encryption is **SRES1** is sent to the recipent as shown on figure 4, ref. Num 405 .(See also figure 4, ref. Num 405, SRES1]

Applicant's second argument is regarding the independent claims 1, 13,16 and 18

Applicant wrote the following in support of his second argument,

"Aura requires the value of RAND2 (which is unknown to the mobile station) to be sent in the clear as depicted in figure 4. This stands in contrast to the Applicants' use of encryption, where the message transmitted from sender to recipient is $Encrypt_k$(Message, Expected-Nonce, New-Nonce). Under an encryption scheme such as claimed by the Applicants, where both parties know the key, K. the recipient can decrypt the message to learn the value of both the Message and the New-Nonce. Thus Aura fails to teach or suggest a method in which at least two nonce values are transmitted in an encrypted message as claimed in Applicants' independent claims 1, 13, 16 and 18."

Examiner disagrees with this argument.

In response to the above argument by the applicant, the examiner response discussed previously is also valid towards this argument.

Therefore examiner asserts that the rejection is valid and clarifies the rejection as follows to show how the each and every limitation of the independent claims **is anticipated by Aura.**

The limitation discussed below is the exact word-by-word limitation cited on the independent claim.

Aura discloses a secure method of transmitting a message between a sender node [figure 4, reference HLR/AUC; authentication station] and a recipient node [figure 4, reference 407; Mobile station] within a network collaboration group, the sender and the recipient sharing a secret encryption key [Ki] (**ki, used in the function Hi meets the recitation of the encryption key which is shared at both authentication center and mobile station**) and an expected nonce value [RAND1] (**the nonce value as described in the disclosure is just a number so RAND1 or random number meets the recitation of the expected nonce value**) comprising:

Generating a new nonce value [RAND 2] known to the sender [Figure 4, reference 404; RAND2] (**The authentication center generate a new nonce value RAND2 at the authentication center/sender**)

Encrypting the message including the expected nonce value and the new nonce value, using the encryption key[See figure 4, reference 405 and H1] (**Both the new nonce value RAND 2 which is generated at the sending station, the expected nonce value RAND1 are encrypted by the key Ki using the hash function H1**];

Transmitting the encrypted message [SRES1] from the sender Figure 4, reference 405] to the recipient [Figure 4, reference 407]; and

verifying, by the recipient, that the encrypted message[SRES1] includes the expected nonce value[figure 4, reference "408"] (**If the encrypted message SRES1 sent from the sender side 405 to the recipient side 407 does not include the corrected expected nonce value RAND1 then the verification test at figure 4, reference 408 fails Since SRES1' will not be equal to SRES1 otherwise it will passé the verification test**).

Applicant's next argument is regarding the dependent claims.

Applicants argued that since the independent claims are patentable therefore all the claims dependent thereon are also in condition for allowance for the same reasons argued for the independent claims.

In response to the above argument by the applicant, the examiner response discussed to the independent claims above is also valid towards this argument because contrary to the applicant's argument, all elements of the independent claims are disclosed by the primary reference as discussed/shown above. Therefore all the elements of the limitations are explicitly or implicitly suggested and disclosed by the reference/s on the records and the rejection remains valid unless the claims are amended be able to overcome the rejection, with out introducing new matter.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. **Claims 1, 12-14,16-18** are rejected under 35 U.S.C. 102(e) as being anticipated by **Tuomas Aura .** (hereinafter referred as **Aura**) (U.S. Patent No: 6, 711, 400 B1)

5. **As per claims 1, 13-14, 16-18** **Aura** a secure method of transmitting a message between a sender node [figure 4, reference HLR/AUC; authentication station] and a recipient node [figure 4, reference 407; Mobile station] within a network collaboration group, the sender and the recipient sharing a secret encryption key [Ki] (**ki, used in the function Hi meets the recitation of the encryption key which is shared at both authentication center and mobile station**) and an expected nonce value [RAND1] (**the nonce value as described in the disclosure is just a number so RAND1 or random number meets the recitation of the expected nonce value**) comprising:

Generating a new nonce value [RAND 2] known to the sender [Figure 4, reference 404; RAND2] (**The authentication center generate a new nonce value RAND2 at the authentication center/sender**)

Encrypting the message including the expected nonce value and the new nonce value, using the encryption key[See figure 4, reference 405 and H1] (**Both the new nonce value RAND 2 which is generated at the sending station, the expected nonce value RAND1 are encrypted by the key Ki using the hash function H1**];

Transmitting the encrypted message [SRES1] from the sender Figure 4, reference 405] to the recipient [Figure 4, reference 407]; and

verifying, by the recipient, that the encrypted message[SRES1] includes the expected nonce value[figure 4, reference "408"] (**If the encrypted message SRES1 sent from the sender side 405 to the recipient side 407 does not include the corrected expected nonce value RAND1 then the verification test at figure 4, reference 408 fails Since SRES1' will not be equal to SRES1 otherwise it will passé the verification test**).

6. **As per claim 12 Aura discloses** a secure method of transmitting a message between a sender node and a recipient node as applied to claims above. Furthermore **Aura d**iscloses the method further including receiving a copy of a prior message being transmitted as a replay attack, and rejecting the replay as illicit at least in part because the replay does not contain the current expected nonce value. [figure 4, 408, discard connection]

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 2-11 and 15** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Tuomas Aura .** (Hereinafter referred as **Aura**) (U.S. Patent No: 6, 711, 400 B1)

in view of **Janson et al** (hereinafter referred as **Janson**) (U. S. Patent No. 5, 729, 608) (Provided with IDS)

9. **As per claims 2-3 Aura discloses Aura discloses** a secure method of transmitting a message between a sender node [figure 4, reference HLR/AUC; authentication station] and a recipient node [figure 4, reference 407; Mobile station] within a network collaboration group, the sender and the recipient sharing a secret encryption key [H1 or Ki] (Ki, in the hash function H1 meets the recitation of the encryption key which shared at both authentication center and mobile station) and an expected nonce value [RAND1] (the nonce value as described in the disclosure is just a number so RAND1 or random number 1 meets the recitation of the expected nonce value) comprising:

Generating a new nonce value known to the sender [Figure 4, reference 404] (The authentication center generate a new nonce value RAND2 at the authentication center/sender)(

Encrypting the message including the expected nonce value and the new nonce value, using the encryption key [See figure 4, reference 405 and H1] (Both the new nonce value RAND 2 which is generated at the sending station, the expected nonce value RAND1 and the key message Ki are encrypted by the encrypted using the hash function

H1]; transmitting the encrypted message [SRES1] from the sender Figure 4, reference 405] to the recipient [Figure 4, reference 407]; and verifying, by the recipient, that the encrypted message includes the expected nonce value[figure 4, reference "408"] (If the encrypted message SRES1 sent from the sender side 405 to the recipient side 407 does not include the corrected expected nonce value RAND1 then the verification test at figure 4, reference 408 fails otherwise passes).

- **Aura** does not disclose expressly discloses

Generating a second new nonce value, known to the recipient node; transmitting a secure response from the recipient to the sender by repeating the method of claim 1, but this time using the second new nonce value in place of the new nonce value and using the new nonce value in place of the expected nonce value.

However, in the field of endeavor **Janson** discloses

Generating a second new nonce value, known to the recipient node; transmitting a secure response from the recipient to the sender by repeating the method of claim 1, but this time using the second new nonce value in place of the new nonce value and using the new nonce value in place of the expected nonce value. [figure 2, 202]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to add the features having the recipient providing the authentication information to the sender as per teachings of Janson in to the method as taught by **Aura,** in order to provide a secure communication.[See Janson, column 2, lines 9-11]

10. **As per claims 4-6; 15** the combination of **Aura and Janson discloses discloses** a secure method of transmitting a message between a sender node and a

recipient node as applied to claims above. Furthermore **Janson** discloses the method wherein the sender is a key managing master node and the recipient is a member node of the collaboration group. [column 3,lines 30-42]

11. **As per claims 7-11 the** combination of **Aura and Janson discloses** a secure method of transmitting a message between a sender node and a recipient node as applied to claims above. Furthermore **Janson** discloses the method wherein the method is used with a key-managing master node in order to perform an authentication process for opening a collaboration group session with a new member node. [Column 3, lines 35-37; column 1, lines 41-51; column 4, lines 6-21]

Conclusion

12. **THIS ACTION IS MADE FINAL**. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
12/28/2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100